

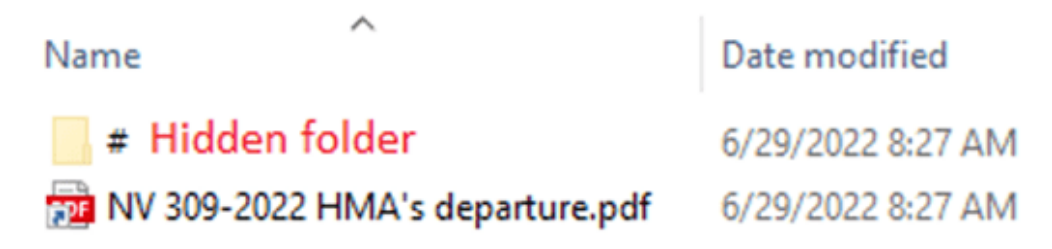
BRONZE PRESIDENT Targets Government Officials

[secureworks.com/blog/bronze-president-targets-government-officials](https://www.secureworks.com/blog/bronze-president-targets-government-officials)

The likely Chinese government-sponsored threat group uses decoy documents and PlugX malware to compromise targets. Thursday, September 8, 2022 By: Counter Threat Unit Research Team

In June and July 2022, Secureworks® Counter Threat Unit™ (CTU) researchers identified a PlugX malware campaign targeting computers belonging to government officials of several countries in Europe, the Middle East, and South America. PlugX is modular malware that contacts a command and control (C2) server for tasking and can download additional plugins to enhance its capability beyond basic information gathering. Several characteristics of this campaign indicate that it was conducted by the likely Chinese government-sponsored BRONZE PRESIDENT threat group, including the use of PlugX, file paths and naming schemes previously used by the threat group, the presence of shellcode in executable file headers, and politically-themed decoy documents that align with regions where China has interests.

The malware is embedded within RAR archive files. Opening the archive on a Windows computer with default settings displays a Windows shortcut (LNK) file (see Figure 1) that masquerades as a document.



Name	Date modified
# Hidden folder	6/29/2022 8:27 AM
NV 309-2022 HMA's departure.pdf	6/29/2022 8:27 AM

Figure 1. Content of RAR archive file. (Source: Secureworks)

Alongside the shortcut is a hidden folder that contains the malware, embedded eight levels deep in a sequence of hidden folders named with special characters (see Figure 2). This tiering is likely to bypass mail-scanning products that may not traverse the entire path when scanning content, suggesting that the delivery mechanism was phishing emails, as there is no other benefit to creating such a folder structure.

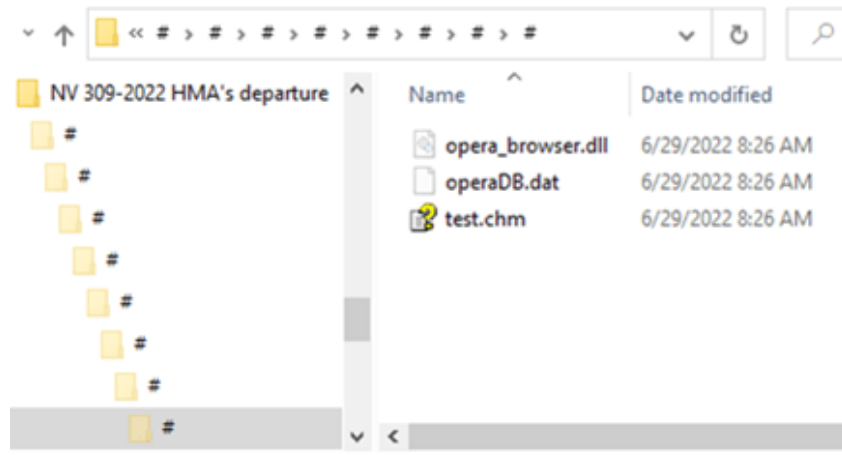


Figure 2. Malicious files contained within hidden folder. (Source: Secureworks)

To execute the malware, the recipient must click the Windows shortcut file. The shortcut executes a renamed legitimate file contained in the eighth hidden folder. Alongside the legitimate file is a malicious DLL and an encrypted payload file. CTU™ researchers observed the malicious payload using the folder names and filenames in Table 1.

Shortcut file	Hidden folder	Legitimate binary	Malicious DLL	Encrypted PlugX payload
HU proposals to the draft EUCO conclusions.pdf.lnk	`	Opera.exe (renamed test.tmp)	opera_browser.dll	operaDB.dat
Embassy of the Republic of Suriname 2022-N-033.pdf.lnk	`	Opera.exe (renamed mail.tmp)	opera_browser.dll	operaDB.dat
Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.pdf.lnk	#	Opera.exe (renamed test.bpl)	opera_browser.dll	operaDB.dat
EL Non-Paper Pandemic Resilience final.docx.lnk	#####	Adobe Stock Photos Cs3.exe (renamed test.chs)	Adobe_Caps.dll	AdobePlugin.dat
313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.pdf.lnk	`	AvastBrowserUpdate.exe (renamed winrar.chm)	Goopdate.dll	AvastDB.dat
EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.pdf.lnk	—	AvastBrowserUpdate.exe (renamed chrom.uce)	Goopdate.dll	AvastDB.dat

Shortcut file	Hidden folder	Legitimate binary	Malicious DLL	Encrypted PlugX payload
NV 309-2022 HMA's departure.pdf.lnk	#	Opera.exe (renamed test.chm)	opera_browser.dll	operaDB.dat

Table 1. Filenames used in PlugX campaign.

The legitimate binary files are vulnerable to DLL search order hijacking. When executed, they import the malicious DLL that loads, decrypts, and executes the payload file. In each sample analyzed by CTU researchers, the shortcut file metadata indicates the file was created on a Windows system either with hostname "desktop-n2v1smh" or "desktop-cb248vr".

Once running, the payload drops a decoy document to the logged-on user's %Temp% directory and copies the three files to a ProgramData subdirectory using the pattern "<Application><3 characters>" (e.g., Operavng) (see Figure 3). This naming scheme has been used in previous BRONZE PRESIDENT PlugX campaigns. CTU researchers observed that when the payload performs the copy operation, it names the legitimate executable with its usual name (e.g., Opera.exe, AdobePlugin.exe, AvastBrowser.exe).

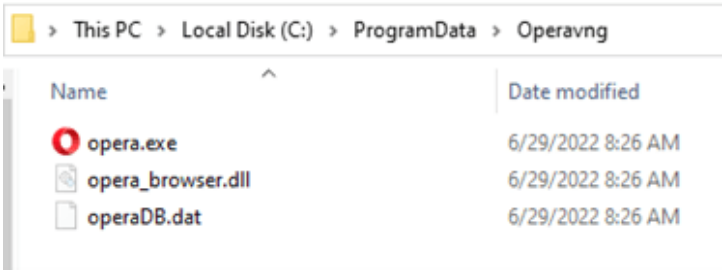


Figure 3. PlugX files copied to ProgramData subdirectory. (Source: Secureworks)

The political nature of the decoy documents suggests that the government officials of various countries are targets for BRONZE PRESIDENT's intelligence collection efforts (see Figures 4, 5, and 6). The threat group consistently targets China's neighbors such as Myanmar and Vietnam. However, its collection requirements can change quickly and are often driven by geopolitical events such as the war in Ukraine.

Note 309/2022

Her Britannic Majesty's Embassy presents its compliments to the Ministry of Foreign Affairs of the Republic of Türkiye and have the honour to refer to NV 247/22 and to inform the Ministry that Sir Dominick Chilcott will depart Ankara on 26 June.

Ms Marianne Young, Deputy Head of Mission, will be Charge d'Affaires until the arrival of Mr Ajay Sharma on 18 June 2022 as referred to in NV 300/22.

Her Britannic Majesty's Embassy avails itself of this opportunity to renew to the Ministry of Foreign Affairs of the Republic of Türkiye the assurance of their highest consideration.



Figure 4. Decoy document used by BRONZE PRESIDENT. (Source: Secureworks)



Embassy of the Republic of Suriname
苏里南共和国大使馆

Bei/2022/06/24-N-033

The Embassy of the Republic of Suriname to the People's Republic of China presents its compliments to the Consular Affairs Department of the Ministry of Foreign Affairs of the People's Republic of China, all Diplomatic Missions, the Offices of the International Organizations of the United Nations System, the Delegation of the European Union, League of Arab States and the African Union in Beijing and with reference to note *Bei/2022/04/029-N-026* dated April 29, 2022 has the honour to communicate the following adjustments:

The Government of the Republic of Suriname has decided to unilaterally exempt the visa requirements for **nationals of all countries** who will travel to Suriname for tourism purposes and family visits.

Figure 5. Decoy document used by BRONZE PRESIDENT. (Source: Secureworks)



Figure 6. Decoy document used by BRONZE PRESIDENT. (Source: Secureworks)

PlugX sets up persistence on the host by setting a registry Run key (see Figure 7).

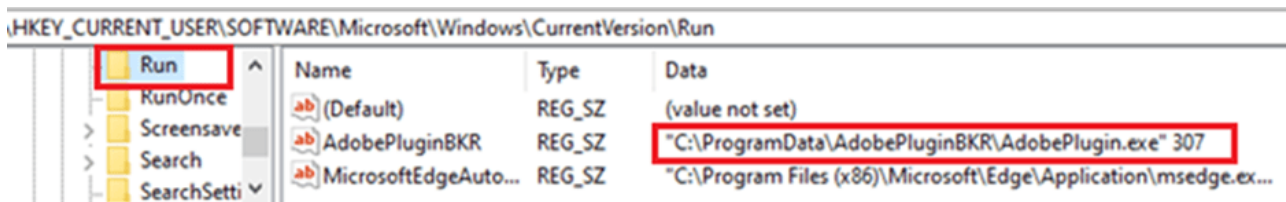


Figure 7. PlugX registry configuration. (Source: Secureworks)

The running instance of the PlugX payload executes the copy of the legitimate file under ProgramData, passing it a command-line argument before exiting (see Figure 8). Passing command-line arguments lets the malware adapt its execution based on its execution location. CTU researchers observed this tactic in previous BRONZE PRESIDENT PlugX campaigns. Once running, the legitimate file again imports the malicious DLL in the same folder, loading, decoding, and passing execution to the malicious payload file.

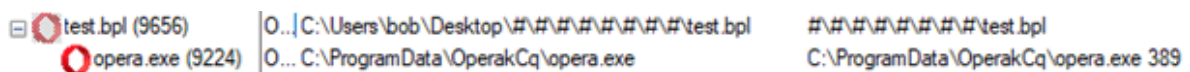


Figure 8. PlugX process execution with command-line argument. (Source: Secureworks)

The payload file calls GetCommandLineW to check the number of arguments. If an additional argument follows the file path, the malware opens the decoy document previously dropped to the user's %Temp% folder and continues execution with its C2 routine.

The malicious DLLs and payloads are heavily obfuscated to hinder analysis and to reduce the likelihood of detection by host-based security software. The malicious DLL executes its payload using an unusual technique. Instead of using a call or jmp instruction, it first decodes and copies the payload to a new allocation of memory and then makes a call to EnumThreadWindows to pass execution to the start of the malicious payload file (see Figure 9).

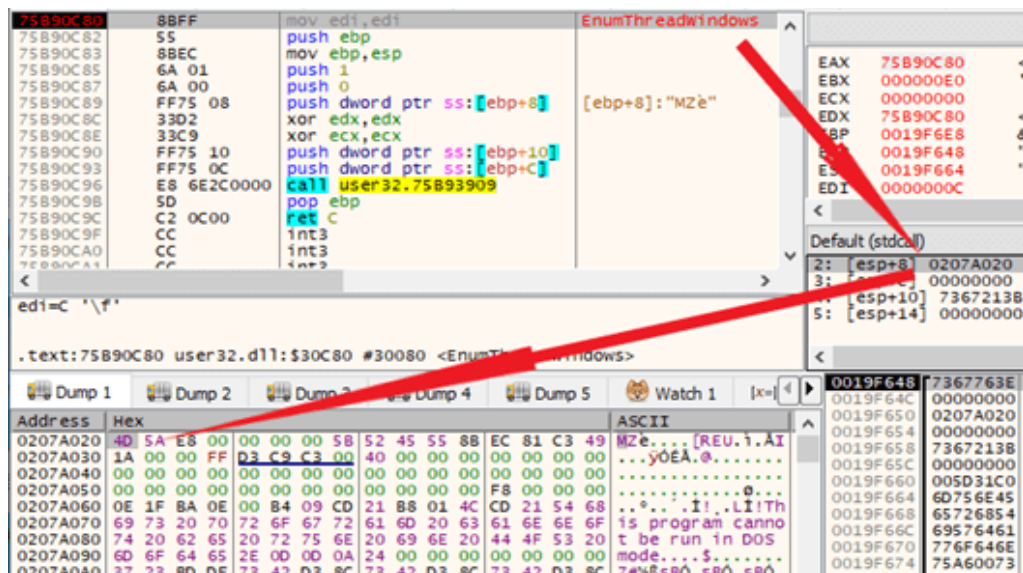


Figure 9. Malicious DLL calling EnumThreadWindows. (Source: Secureworks)

The start of the payload file is treated as executable code in the same way as a Cobalt Strike stageless payload artifact. This could be a tactic developed by BRONZE PRESIDENT to increase the likelihood of its malware being misidentified as the popular Cobalt Strike tool.

The payload resolves various required Windows functions. It then starts a new thread that makes repeated calls to CheckRemoteDebuggerPresent, exiting if it detects a debugger.

Figure 10 shows the payload preparing to decode its configuration. The values pushed to the stack are key length, key, data length, and data address. The key is used as a multibyte XOR value. All observed key value lengths are nine bytes, and their values vary across samples.

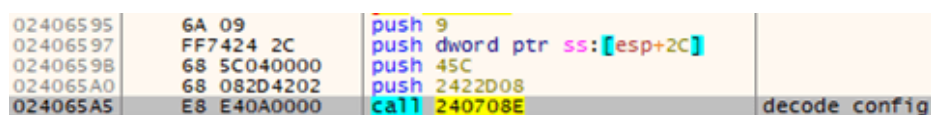


Figure 10. PlugX calling its configuration decode function. (Source: Secureworks)

Figure 11 shows the beginning of the decoded configuration, including the installation directory, mutex name, and the name of the decoy document associated with the sample.

02422CD8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422CE8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422CF8	00 60 28 00	00 60 28 00	00 60 28 00	00 60 28 00	00 00 00 00
02422D08	68 03 00 00	43 0A 00 00	41 00 64 00	6F 00 62 00	6E 00 42 00C...A.d.o.b.
02422D18	65 00 50 00	6C 00 75 00	67 00 69 00	6E 00 42 00	6E 00 42 00e.P.l.u.g.i.n.B.
02422D28	48 00 52 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00K.R.
02422D38	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D48	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D58	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D68	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D78	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D88	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422D98	65 00 50 00	6C 00 75 00	67 00 69 00	6E 00 42 00	6E 00 42 00A.d.o.b.
02422DA8	6C 00 45 00	5A 00 43 00	79 00 00 00	00 00 00 00	00 00 00 00e.P.l.u.g.i.n.B.
02422DB8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00I.E.Z.C.y.
02422DC8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422DD8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422DE8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422DF8	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E08	00 00 00 00	00 00 00 00	74 00 65 00	73 00 74 00	73 00 74 00t.e.s.t.
02422E18	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E28	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E38	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E48	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E58	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E68	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E78	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
02422E88	00 00 00 00	00 00 00 00	45 00 4C 00	20 00 4E 00	20 00 4E 00E.L.N.
02422E98	6F 00 6E 00	2D 00 50 00	61 00 70 00	65 00 72 00	65 00 72 00o.n.-P.a.p.e.r.
02422EA8	20 00 50 00	61 00 6E 00	64 00 65 00	6D 00 69 00	6D 00 69 00P.a.n.d.e.m.i.
02422EB8	63 00 20 00	52 00 65 00	73 00 69 00	6C 00 69 00	6C 00 69 00c.R.e.s.i.l.i.
02422EC8	65 00 6E 00	63 00 65 00	20 00 66 00	69 00 6E 00	69 00 6E 00e.n.c.e.f.i.n.
02422ED8	61 00 6C 00	2E 00 64 00	6F 00 63 00	78 00 00 00	78 00 00 00a.l..d.o.c.x..

Figure 11. PlugX configuration data. (Source: Secureworks)

BRONZE PRESIDENT has demonstrated an ability to pivot quickly for new intelligence collection opportunities. Organizations in geographic regions of interest to China should closely monitor this group's activities, especially organizations associated with or operating as government agencies.

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 2. Note that IP addresses can be reallocated. The IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
c285eaea0fe441f550479f7ef85a3dd0	MD5 hash	Malicious RAR file containing PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.rar)
41d61af1d61d6e1c4718132e64268005ce362b36	SHA1 hash	Malicious RAR file containing PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.rar)
4cd7d84e464a2786446df623629aa7e2e6c776c9a870278eb39b54c5fba05044	SHA256 hash	Malicious RAR file containing PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.rar)

Indicator	Type	Context
3a94449d664033955012edac0161b2b8	MD5 hash	Malicious shortcut file that executes PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.pdf.lnk)
91192be3288369f341951143a81c890c11e23726	SHA1 hash	Malicious shortcut file that executes PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.pdf.lnk)
254739e88ba4b4e62c5e2a313303b4bc679faabe21e7d9c483a2bee846a9dcbc	SHA256 hash	Malicious shortcut file that executes PlugX (Predlog termina zvanicne posjete zamjenice predsjedavajuceg Vijeca ministara i ministarke vanjskih poslova BiH.pdf.lnk)
370557aa593c96533e5994d073ddd202	MD5 hash	Malicious DLL that loads PlugX (opera_browser.dll)
81e8fb5149fda8e1231c9f0f22001cea5b70429b	SHA1 hash	Malicious DLL that loads PlugX (opera_browser.dll)
9adf5dd03388fab2866014d0551881d6e85c7ac94ef5ccf58deb50a83f8a5d50	SHA256 hash	Malicious DLL that loads PlugX (opera_browser.dll)
2a1fc50626afbcc6d8fbda3c65d6cc2b	MD5 hash	Encrypted PlugX payload (operaDB.dat)
c378c0716bf20ebc83403871ae9d96a2717f7599	SHA1 hash	Encrypted PlugX payload (operaDB.dat)
d556d7603178a7e4242c01fa5e490ea4589707eeeab2f3c6c4966bd9b912bd59	SHA256 hash	Encrypted PlugX payload (operaDB.dat)
041a00485779c5a9e42d803e730ceb6c	MD5 hash	Malicious RAR file containing PlugX (Embassy of the Republic of Suriname 2022-N-033.rar)
bd6e5031067724d51abfc2cd2d0fb5ad eed33868	SHA1 hash	Malicious RAR file containing PlugX (Embassy of the Republic of Suriname 2022-N-033.rar)
77a61de438f618fab6e75a920e4ca6756917e501f390b8b4f50c3005505bf488	SHA256 hash	Malicious RAR file containing PlugX (Embassy of the Republic of Suriname 2022-N-033.rar)
3277b31aa055bc149af8c37699019586	MD5 hash	Malicious shortcut file that executes PlugX (Embassy of the Republic of Suriname 2022-N-033.pdf.lnk)

Indicator	Type	Context
d0d6618fc79ffa3de2aec58603539a294a0bc203	SHA1 hash	Malicious shortcut file that executes PlugX (Embassy of the Republic of Suriname 2022-N-033.pdf.lnk)
94e76db201d4998394effae2c132730ff958bf6553f6dd08d0d5856ecb5e8a84	SHA256 hash	Malicious shortcut file that executes PlugX (Embassy of the Republic of Suriname 2022-N-033.pdf.lnk)
675ccbd9318414e2eb0dcabf8a387723	MD5 hash	Malicious DLL that loads PlugX (opera_browser.dll)
89f187c9f76d8afa2b6a8c54fa0bc10563e0169b	SHA1 hash	Malicious DLL that loads PlugX (opera_browser.dll)
abea565d16ec5724591331d962d5cf0237f4628f8cb21b96592c09cc002b10c2	SHA256 hash	Malicious DLL that loads PlugX (opera_browser.dll)
5d71c482148a76900888c8e1d382d413	MD5 hash	Encrypted PlugX payload (operaDB.dat)
6637e077ea52dc62cd31b1a868b3c222953b8aa9	SHA1 hash	Encrypted PlugX payload (operaDB.dat)
02375309e74e91b96c0a41f577f3e4b994f3b406abe0619ee6ad69d00e810093	SHA256 hash	Encrypted PlugX payload (operaDB.dat)
0e37ed727cdb8ae96a50df6391991cc1	MD5 hash	Malicious RAR file containing PlugX (HU proposals to the draft EUCO conclusions.rar)
5285fedf930ccb1acf418c52d581e535504aac76	SHA1 hash	Malicious RAR file containing PlugX (HU proposals to the draft EUCO conclusions.rar)
cbc2d11cb9a495d4697c783cd2aa711a5691d3c257ddb95960d27c96f62c15c1	SHA256 hash	Malicious RAR file containing PlugX (HU proposals to the draft EUCO conclusions.rar)
788cf16121782b4358dc8350012470ab	MD5 hash	Malicious shortcut file that executes PlugX (HU proposals to the draft EUCO conclusions.pdf.lnk)
63d63b96ef50a4002d3acf8f50bc2b62d1ec46c4	SHA1 hash	Malicious shortcut file that executes PlugX (HU proposals to the draft EUCO conclusions.pdf.lnk)
3cdd37d2459779bd17dd47d4dd7f0df6fc59f5208b67b4e4a259c98d8b4788d9	SHA256 hash	Malicious shortcut file that executes PlugX (HU proposals to the draft EUCO conclusions.pdf.lnk)
3e004dd25b5e836bc2500098c55a2b6d	MD5 hash	Malicious DLL that loads PlugX (opera_browser.dll)
602a80e0924a65316cafc48356fe527e427c291f	SHA1 hash	Malicious DLL that loads PlugX (opera_browser.dll)

Indicator	Type	Context
7c29f4a79f74f8b299fb9e778322b002 21e9992d0ac6d2bd915da6629516fa2f	SHA256 hash	Malicious DLL that loads PlugX (opera_browser.dll)
5536783ddc6c15e3e8aef2a756536020	MD5 hash	Encrypted PlugX payload (operaDB.dat)
0809275ecacd52869b43bf4e9804e309 c6bb00b7	SHA1 hash	Encrypted PlugX payload (operaDB.dat)
910c0e5532a94856e8c9047e8c951e21 345bec4ca6b6950cc5ef0da102d2efab	SHA256 hash	Encrypted PlugX payload (operaDB.dat)
0e91279b5f7f732106077ab10aa08c58	MD5 hash	Malicious RAR file containing PlugX (EL Non-Paper Pandemic Resilience final.rar)
b4aa56abac4a19aedcda87ef2fb7c8bb beb3bf64	SHA1 hash	Malicious RAR file containing PlugX (EL Non-Paper Pandemic Resilience final.rar)
4bbb10842941e9004c5449966fca1648 491618ec7841e6befd3e848d75407a10	SHA256 hash	Malicious RAR file containing PlugX (EL Non-Paper Pandemic Resilience final.rar)
1f47ba7fd131a1a6f7623d76b420d7e9	MD5 hash	Malicious shortcut file that executes PlugX (EL Non-Paper Pandemic Resilience final.docx.Ink)
07c5e675714a1af618d8eb1f370be127 63138343	SHA1 hash	Malicious shortcut file that executes PlugX (EL Non-Paper Pandemic Resilience final.docx.Ink)
bf46f4724e5a3b05130df40142446840 33feadb1c10d8309b7e3069a4b014a88	SHA256 hash	Malicious shortcut file that executes PlugX (EL Non-Paper Pandemic Resilience final.docx.Ink)
7c3a5bbbf53d4eb91cd174527460824	MD5 hash	Malicious DLL that loads PlugX (Adobe_Caps.dll)
a6b2c6052ee686e204ad0fbe8d314985 57a3f4ad	SHA1 hash	Malicious DLL that loads PlugX (Adobe_Caps.dll)
840426f9d4d9eb535f5963f76f7cdf84 de084f352dfc0ebc7332b2b4827782e7	SHA256 hash	Malicious DLL that loads PlugX (Adobe_Caps.dll)
459b4b1edd018ba31242b4780ec39a78	MD5 hash	Encrypted PlugX payload (AdobePlugin.dat)
f8ae9ea9ca603dfc10a309b052dc57ee 0b75021d	SHA1 hash	Encrypted PlugX payload (AdobePlugin.dat)
545e2c9965dc0449bb652ae2fb3d1f74 3741ce4f18c045dc50a3f571a1f267f5	SHA256 hash	Encrypted PlugX payload (AdobePlugin.dat)

Indicator	Type	Context
493cb5056dee306ac2c93af2285ad9d8	MD5 hash	Malicious RAR file containing PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.rar)
dcc6edf9c40f9c3f914416805252e11a ecb2e5ad	SHA1 hash	Malicious RAR file containing PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.rar)
325736437e278bccd6f04e0c57f72be7 e1b4787b10743d813581cfc75dc4888f	SHA256 hash	Malicious RAR file containing PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.rar)
f6b365fad2dba5c7378df81339bb3078	MD5 hash	Malicious shortcut file that executes PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.pdf.lnk)
710bc29b56da533cae0ed5bba47916b8 11479ee8	SHA1 hash	Malicious shortcut file that executes PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.pdf.lnk)
eab73a44642e130091177ed2a7938c67 d2411ccf81141a96bdb5116678ac97c2	SHA256 hash	Malicious shortcut file that executes PlugX (313615_MONTENEGRO-2021-HUMAN-RIGHTS-REPORT.pdf.lnk)
5c56ac14f1245fecc7fa930bb49a0f7d	MD5 hash	Malicious DLL that loads PlugX (goopdate.dll)
95f0de261ff57e67d666277b86783650 89853d45	SHA1 hash	Malicious DLL that loads PlugX (goopdate.dll)
b7f6cf8a6a697b254635eb0b567e2a89 7c7f0cefb0c0d4576326dc3f0eb09922	SHA256 hash	Malicious DLL that loads PlugX (goopdate.dll)
c94f930fee694db7253e7784ca3adc87	MD5 hash	Encrypted PlugX payload (AvastDB.dat)
04afecffaaff12058e07bcbda65dbbb6 1cdea762	SHA1 hash	Encrypted PlugX payload (AvastDB.dat)
13e60a836d64ce6d18059c82c2c0c1a3 af0fce87e16d85f26e4b665d4e24e1b1	SHA256 hash	Encrypted PlugX payload (AvastDB.dat)
e2fe6c54cb4a9a45fbc6f7eb3a9c4fbf	MD5 hash	Malicious RAR file containing PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.rar)

Indicator	Type	Context
85d8da08ba6ce60b9116c0c93f8d8c9e4fa7f24c	SHA1 hash	Malicious RAR file containing PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.rar)
09fc8bf9e2980ebec1977a8023e8a2940e6adb5004f48d07ad34b71ebf35b877	SHA256 hash	Malicious RAR file containing PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.rar)
c004559076a1d21e50477580526f2d9f	MD5 hash	Malicious shortcut file that executes PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.pdf.Ink)
840c535120ed91eb88d32abe6fcc06d5b3053674	SHA1 hash	Malicious shortcut file that executes PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.pdf.Ink)
a693b9f9ffc5f4900e094b1d1360f7e7b907c9c8680abfeace34e1a8e380f405	SHA256 hash	Malicious shortcut file that executes PlugX (EU 31st session of the Commission on Crime Prevention and Criminal Justice United Nations on Drugs and Crime.pdf.Ink)
af7b0e51f1572601889994f36b0a9d7a	MD5 hash	Malicious DLL that loads PlugX (goopdate.dll)
0d7daad1d60f2ed2e23188aab1f3bbabf3ad0b63	SHA1 hash	Malicious DLL that loads PlugX (goopdate.dll)
bda43368b62971b395c8fbcc854b6e9d113b3e26931214568e1df6201c1dfd0c	SHA256 hash	Malicious DLL that loads PlugX (goopdate.dll)
1409c055064becf02ed074b6d0976feb	MD5 hash	Encrypted PlugX payload (AvastDB.dat)
bb9803312d697d4cac5f7a2bec57da73b4d88486	SHA1 hash	Encrypted PlugX payload (AvastDB.dat)
dfa01872aab09f04fcb9eca3653bd0fbc6968d040b12aedb93050d363e964891	SHA256 hash	Encrypted PlugX payload (AvastDB.dat)
d3129539bc1e1c6cce321693be186522	MD5 hash	Malicious RAR file containing PlugX (NV 309-2022 HMA's departure.pdf.rar)

Indicator	Type	Context
d640592b13b6983a38948f733a4b4621cdaf2530	SHA1 hash	Malicious RAR file containing PlugX (NV 309-2022 HMA's departure.pdf.rar)
69ba51fe80ef91fb0b7280d16290a24941d3a131cee43f4379821f44d089d63e	SHA256 hash	Malicious RAR file containing PlugX (NV 309-2022 HMA's departure.pdf.rar)
07e9c84bee28450b1ec24a6f06016802	MD5 hash	Malicious shortcut file that executes PlugX (NV 309-2022 HMA's departure.pdf.lnk)
4d15d67e1175f36be7b14c9474102d0982ea97b8	SHA1 hash	Malicious shortcut file that executes PlugX (NV 309-2022 HMA's departure.pdf.lnk)
924fffea4d0a4710d71b507523d76a854f06d4b9e64eb9074c04e1ec34141a53	SHA256 hash	Malicious shortcut file that executes PlugX (NV 309-2022 HMA's departure.pdf.lnk)
a510e7b3e447a090cd3f41c4a1a9bd3a	MD5 hash	Malicious DLL that loads PlugX (opera_browser.dll)
d30791be1bf9d2247faa6dfbeb9c132e9990b401	SHA1 hash	Malicious DLL that loads PlugX (opera_browser.dll)
023d3bce6f1bcf6c15eb839a4e28c4888a346beaad74afce50cf30f4d911e70d	SHA256 hash	Malicious DLL that loads PlugX (opera_browser.dll)
e819924ea9fa0c53634b306648cb9a84	MD5 hash	Encrypted PlugX payload (operaDB.dat)
70f36366b579ba344f9e90ec63b0e273fe6526e0	SHA1 hash	Encrypted PlugX payload (operaDB.dat)
4b7c37ca79536f2692c64dfdc1b70738ceeb74ef7ba9e78d8f8db1dfa7ea64ef	SHA256 hash	Encrypted PlugX payload (operaDB.dat)
64.34.205.41	IP address	PlugX C2 server
69.90.190.110	IP address	PlugX C2 server
104.255.174.58	IP address	PlugX C2 server

Table 2. Indicators for this threat.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team.



Stay Informed

Get the latest in cybersecurity news, trends, and research

SEND ME UPDATES

Secureworks Taegis™

Security Analytics +
Human Intelligence
Delivers Better
Security Outcomes

About Taegis



Latest Report

Reports

2022 State of the Threat Report

